

DFARS Case 2008-D028

Safeguarding Unclassified Information

Roger Nebel
Defense Group, Inc.
roger.nebel@defensegp.com
202.457.7362

Proposed DFARS 252.204-7xxx

Definitions. As used in this clause –

“Adequate security” means that **protection measures** applied are commensurate with the **risks** (i.e., **consequences** and their **probability**) of loss, misuse, or unauthorized access to or modification of information.

Reporting requirement. The contractor shall **report** to the Defense Cyber Crime Center’s (DC3) DoD-DIB Collaborative Information Sharing Environment (DCISE)...**within 72 hours of discovery** of any cyber intrusion events that affect DoD information resident on or transitioning the Contractor’s unclassified information systems.

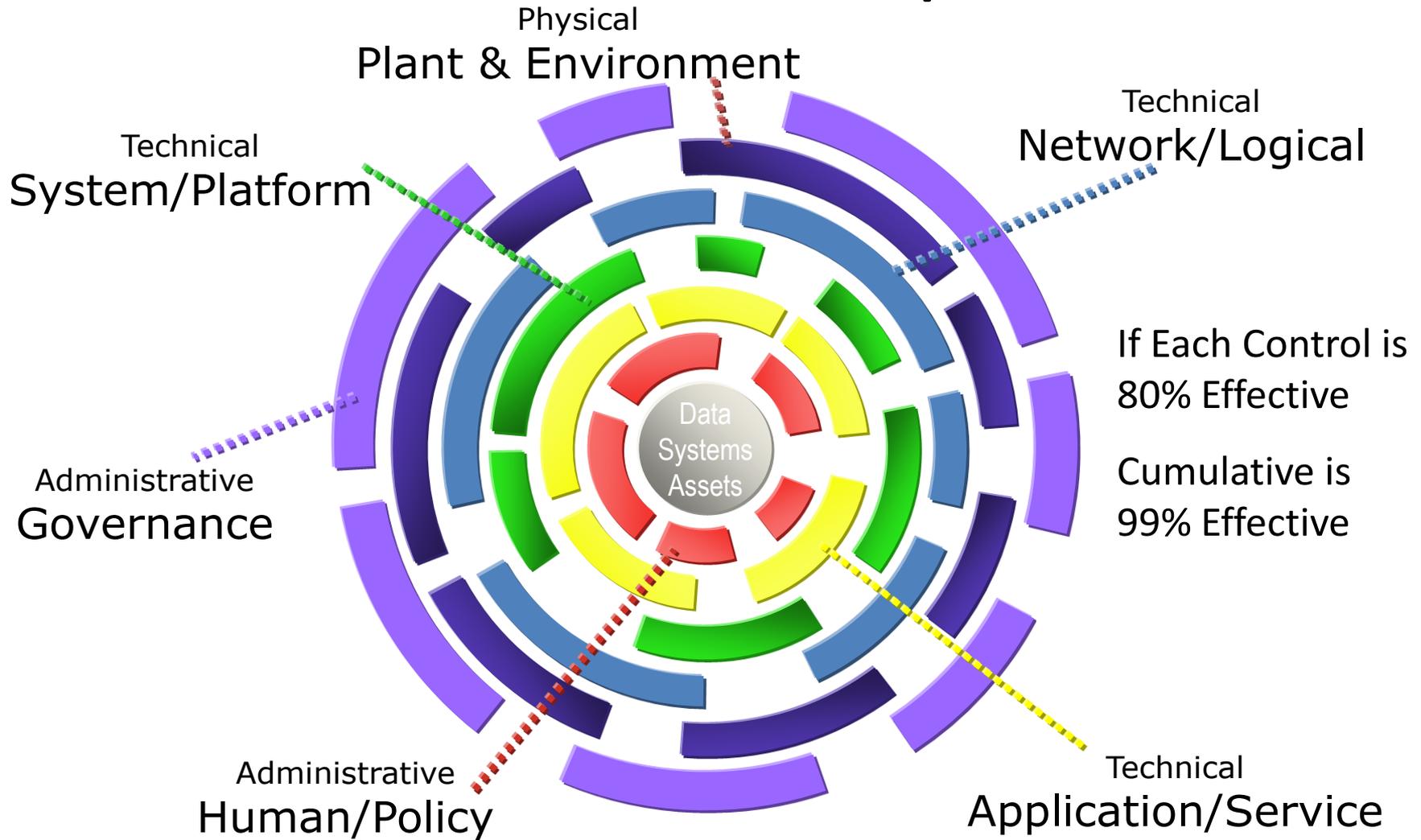
Assessing Risk

- Consequences
 - Financial Loss
 - Loss of Confidentiality, Integrity, Availability
 - Damage to US government interests and/or assets
- Probability
 - Quantitative
 - e. g., 20% chance of \$1m loss, 100 year flood, etc.
 - Precision does not necessarily connote accuracy
 - Qualitative
 - e. g., High Probability, Critical Gap, Gross Negligence, etc.

Controls

- Protection Measures
 - i. e., Safeguards, Controls
- Examples
 - Internet Firewall
 - Background Checks
 - Logging, Monitoring, and Auditing
 - Guns, Guards, and Gates
 - Malicious Software (Malware) Controls

Provide Controls in Depth



Industry Best Practices Examples

- FTC Safeguards Rule (final Rule May 23, 2002)
 - Risk & Controls Assessment
- NIST 800-37 Revision 1 (February 2010)
 - Risk Management Framework
- NIST 800-53 rev 3 (September 2009)
 - Recommended Security Controls
- ISACA COBIT
 - Controls-based Commercial Governance Model
- ISO 27001
 - International Management Model
- PCI DSS
 - Specific Mandatory Controls

Industry Best Practices Examples

- 40+ States + DC Have Mandatory Notification Laws Involving Disclosure of Personally Identifiable Information (PII):
 - Generally Require Timely Public Disclosure of a Breach where PII has been Exposed
 - Most Exempt PII that was Encrypted
 - Many Allow Law Enforcement to Delay Notification During Investigation
- GLBA Mandates Notification for Financial Institutions

